WHAT IS CLAIMED IS:

1. A cryptographic system, comprising:

at least one process;

two or more master keys of which at least one master key is a most-secure master key and requiring a multi-part construction to be exposed, relative to the at least one most-secure master key each of the remaining one or more master keys is a less-secure master key and requiring construction from fewer parts to be exposed, the at least one most-secure master key can be used for detecting tampering of any less-secure master key; and

means for cryptographically linking one or more of the at least one most-secure master key with one or more less-secure master keys such that any tampering of the one or more less-secure master keys can be detected.

2. A cryptographic system as in claim 1, wherein the cryptographic linking is performed by creating a message digest of the one or more most-secure master keys concatenated with the one or more less-secure master keys, and saving the result in a database.

3. A cryptographic system as in claim 1, wherein the cryptographic linking is performed by creating a message digest of the one or more most-secure master keys concatenated with a random value and further concatenated with the one or more less-secure master keys, and saving the result in a database.

4. A cryptographic system as in claim 3, wherein the random value is a Salt.

5. A cryptographic system as in claim 1, wherein for each of the one or more most-secure master keys the cryptographic linking is performed by using that most-secure master key as a

symmetric encryption key, to compute a symmetric message authentication code, and retaining some or all of the result.

6. A cryptographic system as in claim 1, wherein for each of the one or more most-secure master keys the cryptographic linking is performed to produce an 8-byte result by using that most-secure master key as a symmetric encryption key, to compute a symmetric message authentication code, and retaining a 4-byte portion of the result.

7. A cryptographic system as in claim 6, wherein the symmetric message authentication code is computed using cipher-block chaining (CBC) method of any symmetric encryption algorithm.

8. A cryptographic system as in claim 7, wherein the CBC is performed using a random number as an initialization vector, and wherein the initialization vector is saved along with the result.

9. A cryptographic system as in claim 1, wherein the two or more master keys are kept in non-swappable physical memory.

10. A cryptographic system as in claim 9, wherein the non-swappable physical memory is protected.

11. A cryptographic system as in claim 1, wherein the two or more master keys are kept in virtual memory.

12. A cryptographic system as in claim 1, wherein, respectively, the at least one most-secure master key and the one or more less-secure master keys, include a protection key and an integrity

key, the protection key protecting access to sensitive information and the integrity key ensuring the integrity of the sensitive information.

13. A cryptographic system as in claim 1, wherein the sensitive information is kept in a database.

14. A cryptographic system as in claim 1, wherein the sensitive information can be a public key.

15. A cryptographic system as in claim 1, wherein the means for cryptographically linking is a key repository process for enforcing enterprise policies and policy decisions.

16. A method for linking multiple cryptographic keys, comprising:

instantiating at least one process;

providing two or more master keys of which at least one master key is a most-secure master key and requiring a multi-part construction to be exposed, relative to the at least one most-secure master key each of the remaining one or more master keys is a less-secure master key and requiring construction from fewer parts to be exposed, the at least one most-secure master key can be used for detecting tampering of any less-secure master key; and

instantiating a key repository process that validates and records authorizations to access the two or more master keys, the key repository process cryptographically linking one or more of the at least one most-secure master key with one or more less-secure master keys such that any tampering of the one or more less-secure master keys can be detected.

17. A method as in claim 16, wherein the cryptographic linking is performed by creating a message digest of the one or more most-secure master keys concatenated with the one or more less-secure master keys, and saving the result in a database.

18. A method as in claim 16, wherein the cryptographic linking is performed by creating a message digest of the one or more most-secure master keys concatenated with a random value and further concatenated with the one or more less-secure master keys, and saving the result in a database.

19. A method as in claim 16, wherein the random value is a Salt.

20. A method as in claim 16, wherein for each of the one or more most-secure master keys the cryptographic linking is performed by using that most-secure master key as a symmetric encryption key, to compute a symmetric message authentication code, and retaining some or all of the result.

21. A method as in claim 16, wherein for each of the one or more most-secure master keys the cryptographic linking is performed to produce an 8-byte result by using that most-secure master key as a symmetric encryption key, to compute a symmetric message authentication code, and retaining a 4-byte portion of the result.

22. A method as in claim 16, wherein the symmetric message authentication code is computed using cipher-block chaining (CBC) method of any symmetric encryption algorithm.

23. A method as in claim 16, wherein the CBC is performed using a random number as an initialization vector, and wherein the initialization vector is saved along with the result.

24. A method as in claim 16, wherein the two or more master keys are kept in non-swappable physical memory.

25. A method as in claim 23, wherein the non-swappable physical memory is protected.

26. A method as in claim 16, wherein the two or more master keys are kept in virtual memory.

27. A method as in claim 16, wherein, respectively, the at least one most-secure master key and the one or more less-secure master keys, include a protection key and an integrity key, the protection key protecting access to sensitive information and the integrity key ensuring the integrity of the sensitive information.

28. A method as in claim 16, wherein the sensitive information is kept in a database.

29. A method as in claim 16, wherein the sensitive information can be a public key.